

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MAINE**

IN THE MATTER OF THE SEARCH OF  
129 BEAN STREET, TURNER, MAINE  
AND A 2004 BLUE TOYOTA PRIUS WITH  
MAINE REGISTRATION 6504ZY AND VIN  
JTDKB20U140052101

No. 2:24-mj-22-KFW

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41  
FOR A WARRANT TO SEARCH AND SEIZE**

I, Emily Spera, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 129 Bean Street, Turner, Maine, hereinafter “Subject Location,” and a 2004 Blue Toyota Prius, hereinafter the “Subject Vehicle” further described in Attachment A as the “PREMISES”, for the things described in Attachment B.

2. I am a U.S. Postal Inspector with the United States Postal Inspection Service assigned to the Boston Division. I have been a Postal Inspector for ten years. Among my assignments are the investigation of violent crimes including robbery of U.S. Postal Service (USPS) employees, assaults, and burglaries of USPS facilities. I have been trained in all aspects of investigations relating to the U.S. mails at the Postal Inspection Service Training Academy in Potomac, Maryland. I have also completed investigative courses sponsored by the U.S. Postal Inspection Service which focused upon violent crime investigations involving postal employees and its facilities.

3. This affidavit is intended to provide the facts necessary for a determination of probable cause for the requested search warrant.

### **PROBABLE CAUSE**

4. I hereby adopt and incorporate by reference my affidavit filed in support of a criminal complaint charging defendants LANCE FUNDERBURK and WINSTON MCLEOD with conspiracy to rob postal carriers and burgle post offices, in violation of 18 U.S.C. §§ 357, 2114, and 2115, currently pending under case number 2:24-mj-00012-KFW, and attached hereto as Exhibit 1.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that LANCE FUNDERBURK and WINSTON MCLEOD, and others known and unknown, have violated provisions of 21 U.S.C. §§ 846 and 841(a)(1) prohibiting the distribution of controlled substances. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, or fruits of these crimes as further described in Attachment B.

#### **A. 129 Bean Street, Turner and 2004 Blue Toyota Prius**

6. As detailed in Exhibit 1, two cellular phones were recovered from the Paris Post Office, which investigators believed to belong to MCLEOD based, in part, on the fact that his image appeared on the lock screen of one of the devices. Subsequent to their recovery, law enforcement obtained judicially authorized warrants to search MCLEOD's devices. I have conferred with the officer who conducted the search and analysis of MCLEOD's devices, and I have read written analysis produced by the officer, from which I have learned the following, in substance and in part:

a. MCLEOD's phone assigned call number 201-247-0806 (the "Subject Phone") contained an electronic message conversation between it and a contact listed as "Britney Spears" and assigned call number 207-779-4267 (the "Spears Phone"), which I believe is related to the sale of illegal drugs and a vehicle used to transport

illegal drugs, the Subject Vehicle. Throughout the text conversation, this contact was often referred to as "P." An excerpted summary of relevant texts sent and received between the Subject Phone and the Spears Phone is as follows:<sup>1</sup>

<b>Date</b>	<b>Subject Phone</b>	<b>Spears Phone</b>
12/15/23	P I need you to get 28 of the ice ready for me	
12/21/23	P what I'm trying to figure out is If you got my car what the hell are you worried about you have License in stash pot	
12/27/23		Am I supposed to show him how to use the stash
12/28/23	Yeah he was but I can't have him fucking my car up it's important to all of us	
12/28/23	P that's not why you fucked up you fucked us because you been smoking carelessly and not staying on top of your shit. There is no excuse. I help you with your bills and your making 1,300 off of 8 grams. I know because I'm getting that from you now so there isn't no excuses. Iv been bussing my ass to help you as much as possible and still was giving you free Shit	
1/3/24	When I got this car I was for one thing only P and that thing was doing what I'm doing now I told I'll allow you to use the car on down time	

---

<sup>1</sup> Note that all grammar, spelling, and similar errors are reprinted here from the original messages.

1/3/24		I paid title registration n insurance  Ez pass
1/12/24		129 Bean Street Turner

b. After identifying the above message chain, the officer who analyzed the Subject Device also searched for the number of the Spears Phone through law enforcement databases, and was able to identify an individual named PETRAH JACQUES associated with the Spears Phone.

c. The officer searched for vehicles registered to JACQUES, identifying one current vehicle, a Blue 2004 Toyota Prius. The registration address for this vehicle is 129 Bean Street, Turner, Maine, the same address the Spears Phone messaged the MCLEOD Device, as reflected above.

7. I conducted an attorney proffer with FUNDERBURK on about January 26, 2024. I understand that FUNDERBURK proffered with the government in order to obtain leniency at sentencing on his pending federal case. Among other things, I learned the following from FUNDERBURK, in substance and in part:

a. FUNDERBURK admitted that he and MCLEOD had robbed the two postal carriers, and burgled the two post offices as described in Exhibit 1. FUNDERBURK stated that MCLEOD had dropped two cellular phones belonging to him during the burglary of the Paris post office, one of which was a personal phone, and the other was a phone he used to conduct drug trafficking.

b. MCLEOD was a long-time drug trafficker based in East Orange, New Jersey, who supplied several Maine-based coconspirators with cocaine and



fentanyl; in turn, they would sell the drugs downstream to personal-use level customers. FUNDERBURK was aware of a woman he knew as “Petrah” who lived on Bean Street in Turner. FUNDERBURK believed that Petrah owed MCLEOD \$27,000, at least in part as a result of a “bad cocaine problem.”

c. According to FUNDERBURK, as of Saturday, January 20, 2024, the day of the robberies, there were approximately 400 grams of heroin and 200 grams of cocaine at Petrah’s house. FUNDERBURK was shown a Google Map image of the residence at 129 Bean Street in Turner (pictured below). FUNDERBURK stated that he believed the images reflected the Turner residence of Petrah (i.e., PETRA JACQUES).



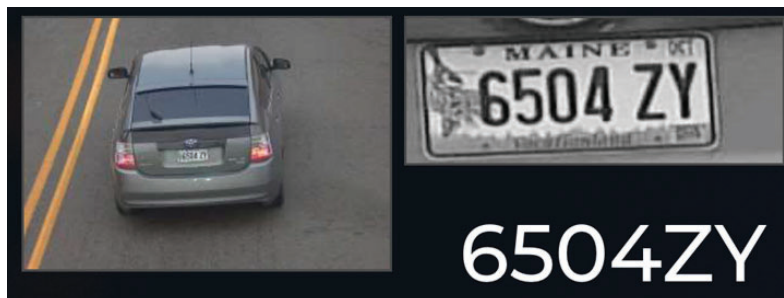
d. FUNDERBURK described Petra’s house as “gray-ish” in color, with a “very nice garage.” FUNDERBURK, who had been inside the residence with MCLEOD, stated that the 2004 Toyota Prius, the Subject Vehicle, would likely be stored in the garage there.

e. FUNDERBURK provided the following additional information about the Subject Vehicle: (a) it likely contained the crowbar that MCLEOD had used to break into the post offices in Paris and North Monmouth; (b) it had a hidden stash

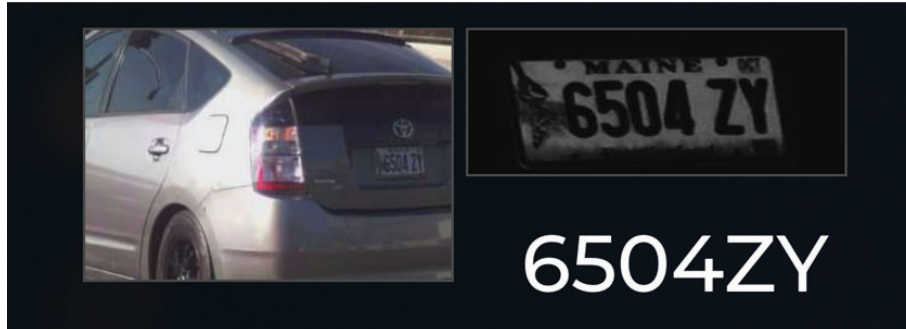
compartment in the middle console that can hold up to three bricks (i.e., kilograms) of narcotics, and likely still contains narcotics; (c) FUNDERBURK has been present in the Subject Vehicle while it was being used to transport narcotics in the stash; and (d) FUNDERBURK knew that the MCLEOD used the Subject Vehicle to transport narcotics from East Orange to various trap houses in Maine for further distribution, utilizing the center console stash to hide the narcotics he was carrying.

8. I have reviewed records relating to 129 Bean Street in law enforcement databases showing that an individual named PETRAH A. JACQUES is associated with that address as recently as October of 2023. Law enforcement databases also reflect that a blue 2004 Toyota Prius with Maine registration 6504ZY and VIN JTDEKB20U140052101, which I believe to be the Subject Vehicle, is registered to 129 Bean Street in Turner.

9. I conducted a license plate query for the Subject Vehicle in the law enforcement database LEARN. It returned nine records for the time period from November 3, 2023, through January 5, 2024, when the Subject Vehicle's license plate was captured on a license plate reader. On January 4, 2024, this image was captured at 237-251 Route 510 in Newark, New Jersey:



10. On November 3, 2023, the following image was captured at 1204 Major Deegan Expressway in the Bronx, New York:



**B. 117 Ash Street in Lewiston, Rear Second Floor Apartment**

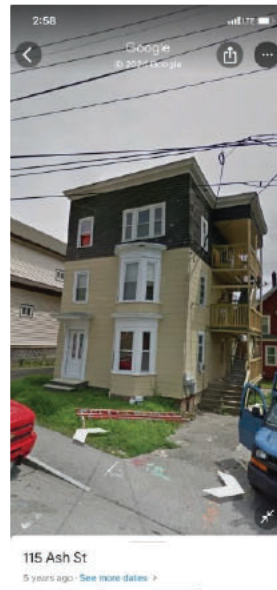
11. Also during FUNDERBURK's attorney proffer, I learned the following information in substance and in part:

a. On December 23, 2023, FUNDERBURK took a bus from Chinatown in New York to Portland, where CC-1 (as identified in Exhibit 1) picked him up at the bus station in Portland and drove him to an apartment located on Ash Street in Lewiston where he stayed on an air mattress in the kitchen for approximately one week.

b. FUNDERBURK stated that the Ash Street apartment was used to traffic heroin, cocaine, meth, and fentanyl. FUNDERBURK was not certain of the exact house number of the Ash Street apartment, because the drug trafficking crew who operated out of the house often provided a false Ash Street address to customers, in order to avoid detection by law enforcement. FUNDERBURK believed the Ash Street apartment to be in the vicinity of house numbers 110, 112, or 116 Ash Street, and affirmed that he would recognize a photograph of the address if he saw it. During the proffer, investigators searched in Google maps for the address "115 Ash St., Lewiston, ME" and the results were shown to FUNDERBURK. He then navigated on Google maps



until he arrived at a building that he positively identified as housing the apartment he described above. A screenshot of that house was captured and is shown below (117 Ash St., Lewiston, ME):



c. FUNDERBURK recalled that the house is located across the street from a church, which 117 Ash Street is. He stated that the apartment is on the second floor, at the top of the stairs it's the apartment in the rear.

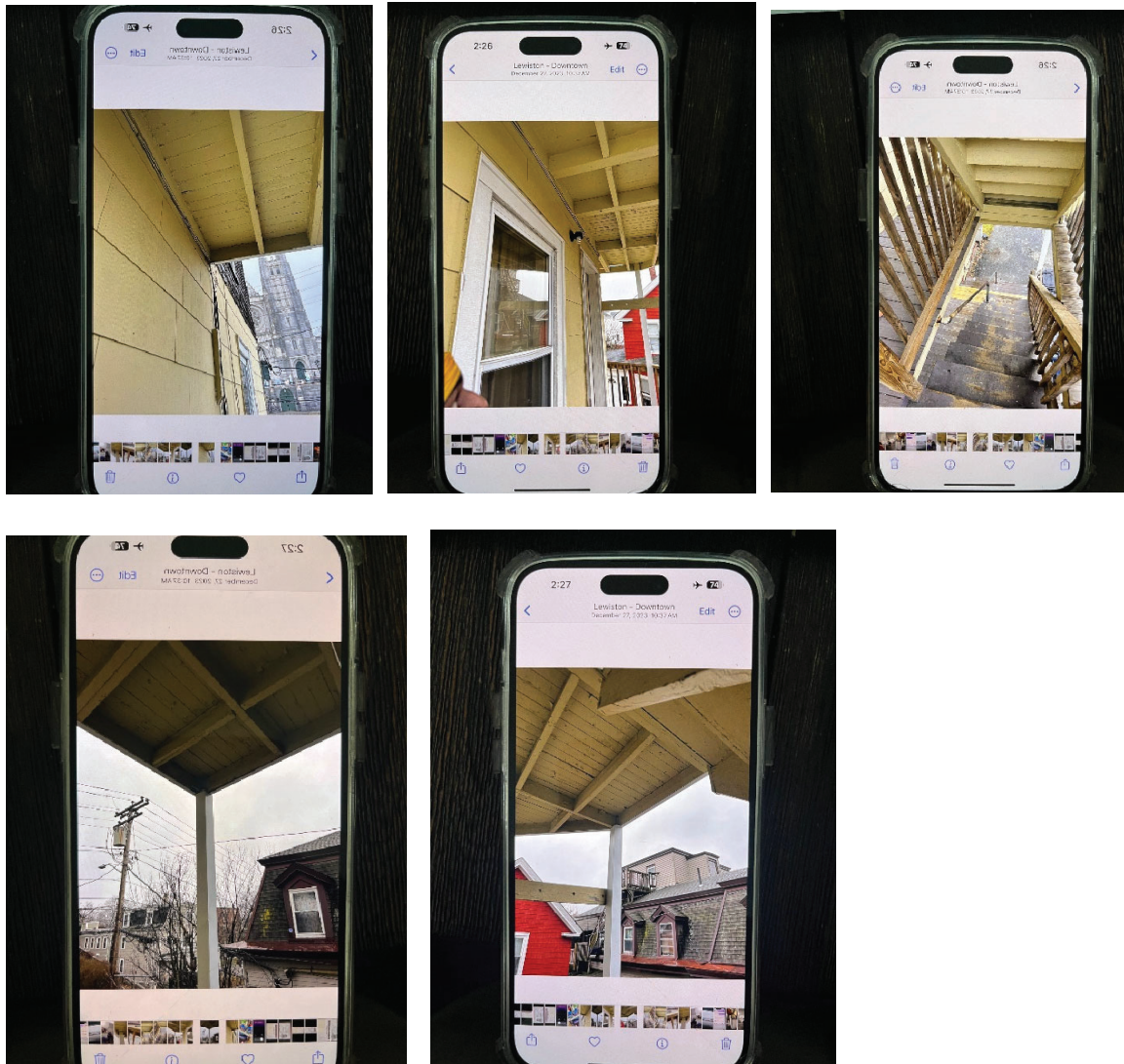
d. FUNDERBURK related a number of instances in December 2023 when he was present in the Ash Street apartment, and observed a significant quantity of drugs in the apartment. On one of his visits to the residence on Ash Street, he recalls a meeting with several coconspirators, one of whom also lived in the Ash Street apartment. That day he recalled seeing a pound of methamphetamine and heroin in the apartment. He also observed heroin and "cut" being put into a blender. FUNDERBURK estimated that approximately \$11,000 worth of narcotics per week is sold through the Ash Street residence; he stated that this trafficking activity was ongoing.



e. FUNDERBURK stated that he goes by “LA,” corresponding to an L.A. Dodgers tattoo on his forearm. Images recovered from the MCLEOD Device were shown to FUNDERBURK during the proffer. He identified the first picture as the inside of the residence at Ash Street in Lewiston. The second picture, he stated, depicted CC-1 cooking crack in the microwave at the Ash Street apartment. The images recovered from the MCLEOD Device and shown to FUNDERBURK appear below:



12. A number of devices were recovered from FUNDERBURK pursuant to his arrest. I conducted a consensual search of one of those devices, pursuant to which I located the two photos above also resident on FUNDERBURK's cellphone. The pictures appear to have been taken on December 27, 2023. I further identified several images of a porch and stairwell that are yellow in color, and which I believe to depict the porch/back stair of 117 Ash Street in Lewiston. Those images appear below:



### **TECHNICAL TERMS**

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

## **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

14. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

15. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.



- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal

information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and

durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

17. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally



speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the

storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

19. Because it is currently unknown whether the Target Subjects are the only individuals to reside at the PREMISES, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

## CONCLUSION

20. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

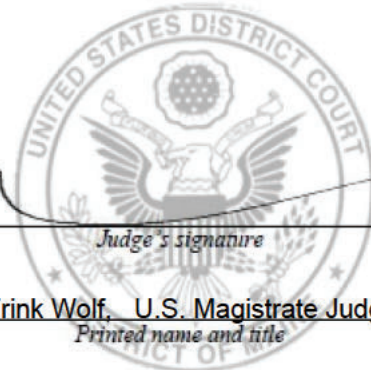


Emily Spera  
U.S. Postal Inspector  
United States Postal Inspection Service

Sworn to telephonically and signed  
electronically in accordance with the  
requirements of Rule 4.1 of the Federal Rules  
of Criminal Procedures

Date: Jan 30 2024

City and state: Portland, Maine



*Judge's signature*

Karen Frink Wolf, U.S. Magistrate Judge  
*Printed name and title*